

FORM-PTO-1390 (Rev. 12-29-99)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY'S DOCKET NUMBER	
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371				032326-161	
				U.S. APPLICATION NO. (if known, see 37 C.F.R. 1.5) Unassigned 09/913884	
INTERNATIONAL APPLICATION NO. PCT/FR00/00130		INTERNATIONAL FILING DATE 20 January 2000		PRIORITY DATE CLAIMED 17 February 1999	
TITLE OF INVENTION METHOD FOR COUNTERMEASURE IN AN ELECTRONIC COMPONENT USING A SECRET KEY ALGORITHM					
APPLICANT(S) FOR DO/EO/US Jean-Sebastien CORON, Nathalie FEYT and Olivier BENOIT					
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:					
1. <input checked="" type="checkbox"/> This is a FIRST submission of items concerning a filing under 35 U.S.C. 371. 2. <input type="checkbox"/> This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371. 3. <input checked="" type="checkbox"/> This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1). 4. <input checked="" type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date. 5. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371(c)(2)) a. <input type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau). b. <input checked="" type="checkbox"/> has been transmitted by the International Bureau. c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US) 6. <input checked="" type="checkbox"/> A translation of the International Application into English (35 U.S.C. 371(c)(2)). 7. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)) a. <input type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau). b. <input type="checkbox"/> have been transmitted by the International Bureau. c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired. d. <input checked="" type="checkbox"/> have not been made and will not be made. 8. <input type="checkbox"/> A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)). 9. <input type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). 10. <input checked="" type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)). 					
Items 11. to 16. below concern other document(s) or information included:					
11. <input checked="" type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98. 12. <input type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included. 13. <input checked="" type="checkbox"/> A FIRST preliminary amendment. <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment. 14. <input type="checkbox"/> A substitute specification. 15. <input type="checkbox"/> A change of power of attorney and/or address letter. 16. <input type="checkbox"/> Other items or information:					

(01/01)

09913884 030802

09/915804

518 Rec'd PCT/PTO 17 AUG 2001

Patent

Attorney's Docket No. 032326-161

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)	
)	
Jean-Sebastien CORON et al)	Group Art Unit: Unassigned
)	
Application No.: Unassigned)	Examiner: Unassigned
)	
Filed: August 17, 2001)	
)	
For: METHOD FOR)	
COUNTERMEASURE IN AN)	
ELECTRONIC COMPONENT)	
USING A SECRET KEY)	
ALGORITHM)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination and the calculation of filing fees, kindly amend the above-identified application as follows.

All references are to the version of the application appearing in the Annex to the International Preliminary Examination Report.

IN THE SPECIFICATION:

Page 1, immediately following the title appearing on lines 1 and 2, insert the following:

--This disclosure is based upon, and claims priority from French Application No.

99/01937, filed on February 17, 1999 and International Application No. PCT/FR00/00130,

filed January 20, 2000, which was published on August 24, 2000 in a language other than English, the contents of which are incorporated herein by reference.

Background of the Invention--

Page 5, between lines 5 and 6, insert the following heading:

--Summary of the Invention--

Page 6, before line 25, insert the following heading:

--Brief Description of the Drawings--

Page 7, before line 18, insert the following heading:

--Detailed Description--

Add the following Abstract:

--A countermeasure method in an electronic component using a secret key algorithm K on an input message M executes an operation $O_{PN}(D)$ on input data D. A random value, of one first random information U, is generated that is of identical size as the input information D. A second random information V, is calculated by performing an exclusive OR operation between the input information and the first random information U. The operation O_{PN} or the sequence of operations are successively executed on the first input information U and to the second random information V, supplying respectively a first random result $O_{PN}(U)$ and a second random result $O_{PN}(V)$.--

IN THE CLAIMS:

Cancel claims 9, 11 and 12.

Kindly replace claims 1-8 and 10, as follows.

1. (Amended) A countermeasure method in an electronic component using a cryptographic algorithm with a secret key K on an input message (M), of the type in which an operation (OPN) or a sequence of operations comprising a bit by bit manipulation of an input data item (D) is executed, in order to supply an output data item (OPN(D)), said operation comprising the following steps:

- drawing a first random data item (U), having the same size as the input data item (D);
- calculating a second random data item (V), by performing an exclusive OR operation between the input data item and the first random data item (U);
- executing the operation (OPN) or the sequence of operations on the first random data item (U) and the second random data item (V), to thereby generate respectively a first random result (OPN(U)) and a second random result (OPN(V)).

2. (Amended) A countermeasure method according to Claim 1, further including the following step:

- calculating the output data item (OPN(D)) by performing an exclusive OR operation between the first and second random results.

3. (Amended) A countermeasure method according to Claim 1 wherein said steps are performed during operations relating to data calculated from the input message.
4. (Amended) A countermeasure method according to claim 1, wherein a new random value (U) is drawn at each new execution of said operation or sequence of operations.
5. (Amended) A countermeasure method according to Claim 1, wherein said steps are performed as part of an operation or a sequence of operations performed on said secret key.
6. (Amended) A countermeasure method according to Claim 5, wherein the cryptography algorithm is carried out in several calculation rounds comprising a sequence of operations on the secret key K in order to supply, at each round, a corresponding subkey (K_i), and wherein said steps are applied to said sequence of operations in order to supply, at each round, a first random result (K_{iY}) and a second random result (K_{iZ}).
7. (Amended) A countermeasure method according to Claim 6, wherein, for each round, the following steps are performed:
- calculating an exclusive OR result between an input data item for that round and the first random result (K_{iY}) in order to supply an intermediate result and;

- calculating an exclusive OR result between said intermediate result and the second random result (K_{iz}) in order to supply an output data item for that round.

8. (Amended) A countermeasure method according to claim 1, wherein a new random value is drawn at each new execution of the cryptography algorithm.

10. (Amended) A countermeasure method according to claim 1, wherein said cryptographic algorithm is the DES algorithm.

13. (New) A countermeasure method according to Claim 5 wherein said steps are performed during operations relating to data calculated from the input message.

14. (New) A countermeasure method according to claim 5, wherein a new random value (U) is drawn at each new execution of said operation or sequence of operations.

15. (New) A countermeasure method according to Claim 6 wherein said steps are performed during operations relating to data calculated from the input message.

16. (New) A countermeasure method according to claim 6, wherein a new random value (U) is drawn at each new execution of said operation or sequence of operations.

17. (New) A countermeasure method according to Claim 7 wherein said steps are performed during operations relating to data calculated from the input message.

18. (New) A countermeasure method according to claim 7, wherein a new random value (U) is drawn at each new execution of said operation or sequence of operations.

19. (New) An electronic security component of the type in which a cryptographic algorithm with a secret key is applied to an input message using bit-by-bit manipulation of an input data item D to calculate an output data item, comprising:

means for generating a first random data item U having the same size as said input data item D;

means for performing an exclusive-OR operation on said input data item D and said first random data item U, to generate a second random data item V; and

means for executing said bit-by-bit manipulation on said first random data item U and said second random data item V to generate a first random result and a second random result.

20. (New) The electronic security component of claim 19, further including means for performing an exclusive-OR operation on said first and second random results to generate said output data item.

21. (New) The electronic security component of claim 19, wherein said cryptographic algorithm comprises a plurality of calculation rounds, and wherein said first and second random results are generated during each calculation round.

22. (New) The electronic security component of claim 21, wherein said executing means performs the following steps during each calculation round:

- calculating an exclusive OR result between an input data item for that round and the first random result in order to supply an intermediate result and;
- calculating an exclusive OR result between said intermediate result and the second random result in order to supply an output data item for that round.

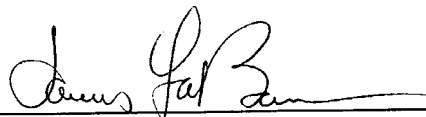
23. (New) The electronic security component of claim 19, wherein said means for generating a first random data item generates a new random data item for each calculation round.

REMARKS

Entry of the foregoing amendment is respectfully requested. This amendment is intended to place the claims in a more conventional format and eliminate the multiple dependency of the claims.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: August 17, 2001

Attachment to Preliminary Amendment dated August 17, 2001

Marked-up Claims 1-12

1. (Amended) A countermeasure method in an electronic component using a cryptographic algorithm with a secret key K on an input message (M), [characterised in that the execution of] of the type in which an operation (OPN) or [of] a sequence of operations comprising a bit by bit manipulation of an input data item (D) is executed, in order to supply an output data item (OPN(D)), [comprises] said operation comprising the following steps:

- drawing a [random value, of a] first random data item (U), [with] having the same size as the input data item (D);
- calculating a second random data item (V), [effecting] by performing an exclusive OR operation between the input data item and the first random data item (U);
- executing the operation (OPN) or the sequence of operations [following on from] on the first random data item (U) and the second random data item (V), [supplying] to thereby generate respectively a first random result (OPN(U)) and a second random result (OPN(V)).

2. (Amended) A countermeasure method according to Claim 1, [also comprising] further including the following step:

- calculating the output data item (OPN(D)) [effecting] by performing an exclusive OR operation between the first and second random results.

Attachment to Preliminary Amendment dated August 17, 2001

Marked-up Claims 1-12

3. (Amended) A countermeasure method according to Claim 1 [or 2, characterised in that it is applied to operations (EXP PERM, P PERM)] wherein said steps are performed during operations relating to data calculated from the input message [(M)].
4. (Amended) A countermeasure method according to [any one of the preceding claims, characterised in that] claim 1, wherein a new random value (U) is drawn at each new execution of [the] said operation or sequence of operations.
5. (Amended) A countermeasure method according to Claim 1, [applied to] wherein said steps are performed as part of an operation or a sequence of operations [(KEY PERM, SHIFT, COMP PERM)] performed on [the] said secret key [(K)].
6. (Amended) A countermeasure method according to Claim 5, wherein the cryptography algorithm [comprising] is carried out in several calculation rounds[, and] comprising a sequence of operations on the secret key K in order to supply, at each round, [(T_i),] a corresponding subkey (K_i), [a method characterised in that it is] and wherein said steps are applied to [the] said sequence of operations in order to supply, at each round, a first random result (K_{iY}) and a second random result (K_{iZ}).

Attachment to Preliminary Amendment dated August 17, 2001

Marked-up Claims 1-12

7. (Amended) A countermeasure method according to Claim 6, wherein, for each round, [(Ti) an exclusive OR operation between the subkey (K_i) and an input data item (1) in order to supply an output data item (b), characterised in that this operation is replaced by the following operations] the following steps are performed:

- calculating [the] an exclusive OR result between [the said] an input data item [(1)] for that round and the first random result (K_{1Y}) in order to supply an intermediate result [(b')] and;

- calculating [the] an exclusive OR result between [the] said intermediate result [(b')] and the second random result (K_{1Z}) in order to supply [the said] an output data item [(b)] for that round.

8. (Amended) A countermeasure method according to [any one of Claims 1, 2, 3, 5, 6 and 7, characterised in that] claim 1, wherein a new random value [(U or Z)] is drawn at each new execution of the cryptography algorithm.

10. (Amended) A countermeasure method according to [any one of the preceding claims, characterised in that it is applied to] claim 1, wherein said cryptographic algorithm is the DES algorithm.

**TRANSLATION OF THE ANNEX
TO THE INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

**A COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT
USING A SECRET KEY CRYPTOGRAPHY ALGORITHM**

5 The present invention concerns a countermeasure method in an electronic component using a secret key cryptography algorithm. They are used in applications where access to services or to data is strictly controlled. Such components have an architecture formed around a microprocessor and memories, including a program memory which contains the secret key.

10 These components are notably used in smart cards, for certain applications thereof. These are for example applications involving access to certain databanks, banking applications, remote payment applications, for example for television, petrol
15 dispensing or passing through motorway tolls.

These components or cards therefore use a secret key cryptography algorithm, the best known of which is the DES algorithm (standing for Data Encryption Standard in British and American literature). Other

secret key algorithms exist, such as the RC5 algorithm or the COMP128 algorithm. This list is of course not exhaustive.

5 In general terms and briefly, the function of these algorithms is to calculate an enciphered message from a message applied at the input (to the card) by a host system (a server, banking dispenser etc) and the secret key contained in the card, and supplying this enciphered message in return to the host system, which
10 for example enables the host system to authenticate the component or the card, to exchange data etc.

The characteristics of the secret key cryptography algorithms are known: calculations made, parameters used. The only unknown is the secret key
15 contained in program memory. All the security of these cryptography algorithms relates to this secret key contained in the card and unknown to the world outside this card. This secret key cannot be deduced solely from knowledge of the message applied as an input and
20 the enciphered message supplied in return.

However, it has become apparent that external attacks, based on current consumptions or a differential current consumption analysis when the microprocessor of a card is running the cryptography
25 algorithm in order to calculate an enciphered message, enable ill-intentioned third parties to find the secret key contained in this card. These attacks are referred to as DPA attacks, the English acronym for Differential Power Analysis.

The principle of these DPA attacks is based on the fact that the current consumption of the microprocessor executing the instructions varies according to the data being manipulated.

5 Notably, when an instruction executed by the microprocessor requires manipulation of data bit by bit, there are two different current profiles depending on whether this bit is "1" or "0". Typically, if the microprocessor manipulates a "0", there is at this time
10 of execution a first consumed current amplitude, and if the microprocessor manipulates a "1" there is a second consumed current amplitude, different from the first.

 Thus the DPA attack exploits the difference in current consumption profile in the card during the
15 execution of an instruction according to the value of the bit manipulated. In simplified terms, conducting a DPA attack consists of identifying one or more particular periods during which the algorithm is run comprising the execution of at least one instruction
20 manipulating data bit by bit; reading a very large number N of current consumption curves during this period or periods, one curve per different message to which the algorithm is applied; predicting, for each curve, the value taken by a bit of the data for an
25 assumption on a subkey, that is to say on at least part of the secret key, which makes it possible to make the prediction; and making a sort of the curves according to the corresponding Boolean selection function; a first packet of curves is obtained for which the
30 prediction is "1" and a second packet of curves for

Notably, the algorithms generally comprise permutations which require such manipulations by the microprocessor. By analysing the current consumption during the execution of these manipulations bit by bit, it is possible to find the value of some bits at least

of the data item manipulated. Knowledge of this data item can supply information on intermediate results obtained during the execution of the enciphering algorithm, which in their turn can make it possible to find at least some of the bits of the secret key used.

Three documents resembling the invention whilst being distinguished from it are cited below.

The first document "NTT Review, Vol. 6, N° 4, of 1 July 1997, pages 85-90, Miyaguchi S: "Secret key ciphers that change the encipherment algorithm under the control of the key", XP000460342", denoted D1, concerns a resolution of a mathematical problem which avoids the known enciphered attacks with a message. The method described modifies the "key schedule", translated by "subpart of the key in the algorithm", of any secret key algorithm. However, this method no longer applies to the standard DES algorithm, a well-known secret key algorithm. The technology described in this document consists of effecting data rotations and also data substitution.

The second document "Institute of Electrical and Electronics Engineers, IEEE Global Telecommunications Conference, Phoenix, Arizona, Nov. 3-8, 1997, vol. 2, 3 November 1997, pages 689-693, Yi X et al: "A method for obtaining cryptographically strong 8X8 S-boxes", XP000737626", denoted D2, concerns a proposal to improve the S-boxes in the standard DES algorithm intended to improve security on a cryptanalysis level, that is to say in mathematics, but not in physical cryptography.

5

10

15

20

25

In this way, the operation or series of operations manipulates only random data items so that it is no longer possible to implement a DPA attack.

5 In order to find the output data item corresponding to the application of the series of steps to the input data item, it suffices to calculate the exclusive OR between the first and second random results.

10 In a first method of applying this countermeasure method, the operation or series of operations relate to a data item calculated from the message to be enciphered.

15 In a second method of applying the countermeasure method according to the invention, this method is applied to operations relating directly to the secret key and supplying, for each round of the algorithm, the subkey to be used.

20 In this method of applying the countermeasure method according to the invention, provision is made for effecting a first series of steps according to the method indicated above so that a first random subkey and a second random subkey are obtained.

25 In this variant, instead of calculating the true subkey for the round in question, these random subkeys are used, so that the true subkey of each round no longer appears in clear: only random subkeys are manipulated.

30 Thus the present invention is distinguished first of all from document D1 in that it concerns solely the DES without modifying its structure, nor its inputs,

nor its data outputs. The XOR operation used described below makes it possible to mask the data with a random parameter.

5 It is also distinguished from document D2 in that it deals with the problems of physical cryptographies, that is to say it sets out to resolve problems of implementation through the appearance of secondary effects; in addition does not concern the S-boxes but
10 deals with the problems of security during compressions, permutations and expansions of data (cf Figure 1 described hereinafter).

Finally, it is distinguished from document D3 in that it uses a random number within the DES algorithm for protecting the execution of the DES against all
15 types of attack.

Other characteristics and advantages of the invention are detailed in the following description given for indication and in no way limitatively, and with reference to the accompanying drawings, in which:

20 - Figures 1 and 2 are detailed flow diagrams of the first and second rounds of the DES algorithm;

- Figure 3 depicts schematically the countermeasure method according to the invention applied to an operation effecting a data manipulation
25 bit by bit;

- Figure 4 depicts a first method of applying the countermeasure method according to the invention in the execution of the DES algorithm;

- Figure 5 depicts schematically the end of
30 execution of the DES algorithm;

- Figure 6 depicts schematically a second method of applying the method according to the invention to the operations of the DES algorithm manipulating the secret key; and

5 - Figure 7 depicts a detailed flow diagram of the DES algorithm in an application of the countermeasure method corresponding to the diagram in Figure 5; and

10 - Figure 8 depicts a block diagram of a smart card in which it is possible to implement the countermeasure method according to the invention.

15 The DES secret key cryptographic algorithm (hereinafter reference will be made more simply to the DES or to the DES algorithm) includes 16 calculation rounds, denoted T1 to T16, as depicted in Figures 1 and 2.

20 The DES begins with an initial permutation IP on the input message M (Figure 1). The input message M is a word f of 64 bits. After permutation, a word e of 64 bits is obtained, which is divided into two in order to form the input parameters L0 and R0 of the first round (T1). L0 is a word d of 32 bits containing the 32 most significant bits of the word e. R0 is a word h of 32 bits containing the 32 least significant bits of the word e.

25 The secret key K, which is a word q of 64 bits, itself undergoes a permutation and a compression in order to supply a word r of 56 bits.

 The first round comprises an operation EXP PERM on the parameter R0, consisting of an expansion and a

permutation, in order to supply as an output a word 1 of 48 bits.

5 This word 1 is combined with a parameter K1, in an operation of the exclusive OR type denoted XOR, in order to supply a word b of 48 bits. The parameter K1, which is a word m of 48 bits, is obtained from the word r by a shift by one position (the operation denoted SHIFT in Figures 1 and 2) supplying a word p of 48 bits, to which an operation is applied comprising a permutation and a compression (the operation denoted
10 COMP PERM).

The word b is applied to an operation denoted SBOX, at the output of which a word a of 32 bits is obtained. This particular operation consists of
15 supplying an output data a taken from a table of constants TC₀ according to an input data item b.

The word a undergoes a permutation P PERM, giving as an output the word c of 32 bits.

This word c is combined with the input parameter
20 L0 of the first round T1, in a logic operation of the exclusive OR type, denoted XOR, which supplies as an output the word g of 32 bits.

The word h (=R0) of the first round supplies the input parameter L1 of the following round (T2) and the
25 word g of the first round supplies the input parameter R1 of the following round. The word p of the first round supplies the input r of the following round.

The other rounds T2 to T16 occur in a similar fashion, except with regard to the shift operation

Each round T_i thus receives as an input the parameters L_{i-1} , R_{i-1} and r and supplies as an output the parameters L_i and R_i and r for the following round T_{i+1} .

10 This calculation of the enciphered message C
comprises in practice the following operations:

- It can be seen that this algorithm comprises many
20 operations manipulating the data bit by bit, like the
permutation operation.

According to the countermeasure method according to the invention, a software countermeasure is applied when the microprocessor which calculates the enciphered message effects a manipulation bit by bit. In this way, the statistical processing and the Boolean selection function of the DPA attack applied to the current consumption curves no longer supplies any information: the signal $DPA(t)$ remains zero whatever the subkey assumptions made.

The software countermeasure according to the invention then consists of making each of the bits manipulated by the microprocessor unpredictable.

5 The principle of this countermeasure is depicted in Figure 3.

Let an input data item be D.

Let there be an operation OPN to be calculated on this input data item D, the result of which is denoted OPN(D). This operation OPN requires a bit by bit
10 manipulation of the input data item D by the microprocessor; it is a case for example of a permutation.

According to the invention, instead of applying the operation OPN to the input data item D in order to
15 calculate the result OPN(D) of the operation, the following different steps are performed:

- drawing a random value for a first random data item U, of the same size as the input data item D (for example 32 bits);
- 20 - calculating a second random data item V by effecting an exclusive OR between the input data item and the first random data item: $V = D \text{ XOR } U$;
- calculating the operation OPN on the first random data item U, giving a first random result
25 OPN(U);
- calculating the operation OPN on the second random data item V, giving a second random result OPN(V);

- calculating the result $OPN(D)$ by effecting an exclusive OR between the first and second random results: $OPN(D) = OPN(U) \text{ XOR } OPN(V)$.

5 This method can equally well be applied to a single operation or to a series of operations.

A first method of applying the countermeasure method according to the invention concerns operations on data calculated from the message (M) to which the algorithm is applied. The input data item D is in this case a data item calculated from the message M.

10 In a practical example of this first method of application of the algorithm DES depicted in Figure 4, this method is applied on the one hand to the operation EXP PERM and on the other hand to the operation P PERM, which both comprise a permutation requiring a bit by bit manipulation of the input data item.

15 In the figure the application of this countermeasure to these operations is denoted $CM(EXP \text{ PERM})$ and $CM(P \text{ PERM})$.

20 The software countermeasure according to the invention then consists of performing, in place of each operation P PERM and EXP PERM, the operations $CM(EXP \text{ PERM})$ and $CM(P \text{ PERM})$ according to the calculation sequence described in Figure 3, using a random variable U. As each round of the algorithm comprises an operation EXP PERM and an operation P PERM, this countermeasure can be applied in each of the rounds of the DES.

25 Experience shows that it is the first three rounds and the last three rounds which allow DPA

attacks. Afterwards, it becomes very difficult or even impossible to predict the bits.

Thus an implementation of a countermeasure method according to the invention which is less expensive in calculation time consists of applying only these first
5 three and last three rounds of the DES.

Different variant applications of the countermeasure method according to the invention concern the drawing of a random value for the first
10 random data item U. Depending on whether or not a great deal of calculation time is available, it is possible to draw a new random value each time, for each of the operations or series of operations for which the countermeasure method according to the invention is
15 implemented.

Thus, in Figure 4, for the operation CM(EXP PERM), a value u1 for the random data item U is drawn and, for the operation CM(P PERM), another value u2 is drawn for the random value U.

20 Or else it is possible to draw a new random value for each round of the algorithm, or a single random value at the start of the algorithm.

The implementation of the countermeasure method according to the invention depends principally on the applications concerned, depending on whether or not it
25 is possible to devote a great deal of additional time to the countermeasure.

A second mode of applying the countermeasure method according to the invention is depicted in Figure
30 6. It concerns more particularly the calculation

operations applied to the secret key K in order to supply each of the subkeys K_i used in the rounds of the algorithm. In the example of the DES, these operations are the following KEY PERM, executed at the start of
5 DES and SHIFT and COMP PERM executed at each round. During these operations, at certain times, the microprocessor separately manipulates a bit of the secret key, therefore leaving the possibility of a DPA attack on this bit.

10 The countermeasure method according to the invention is then applied by protecting the data item, the secret key in this case, before performing these operations, so that it is no longer possible to obtain information by DPA attack.

15 Thus, and as schematically shown in Figure 5, a random value of a first random data item Y is drawn, with the same size as the secret key K. A second random data item Z with the same size is calculated, making an exclusive OR between the secret key K and the
20 first random data item Y: $Z = K \text{ XOR } Y$.

In the example, the sequence of operations comprises the following operations KEY PERM, SHIFT, COMP PERM. Then this sequence of operations is applied to each of the two random data items Y and Z,
25 successively. Thus, from these two data items Y and Z applied successively as an input, the data items Y' , $P_{iy'}$, $K_{iy'}$, or respectively Z' , $P_{iz'}$, $K_{iz'}$ are obtained, at the output of the operations KEY PERM, SHIFT, COMP PERM.

A practical example of an application to the DES is shown in Figure 7.

In the DES, the operation KEY PERM is executed only once, at the start, whilst the sequence of operations SHIFT and COMP PERM is executed in each round.

In addition, the output of the operation SHIFT of a round T_i is applied as an input of the operation SHIFT of the following round T_{i+1} (see Figures 1 and 2).

In order to apply the countermeasure method according to the second mode of application to this DES algorithm, the first operation KEY PERM is then applied to the random data Y and Z, which gives two intermediate random data, denoted Y' and Z' . These two intermediate random data are successively applied to the operations SHIFT of the first round T_1 , supplying two intermediate random data denoted $P_{1Y'}$ and $P_{1Z'}$. These two random data are on the one hand stored in working memory for the operation SHIFT of the following round (the second round), and on the other hand applied successively to the operation EXP PERM of the first round, in order to supply a first intermediate result $K_{1Y'}$ and $K_{1Z'}$.

This procedure is followed in each round. Thus, at each round T_i , a first random result is obtained: $K_{iY'} = \text{EXP PERM} (\text{SHIFT} (Y'))$ and a second random result: $K_{iZ'} = \text{EXP PERM} (\text{SHIFT} (Z'))$;

and the intermediate random data SHIFT (Y')= $P_{iy'}$ and SHIFT (Z')= $P_{iz'}$ are stored in working memory for the following round $Ti+1$.

5 For each round Ti , it would then be possible to recalculate the corresponding subkey K_i corresponding to the sequence of operations KEY PERM, SHIFT and COMP PERM of this round applied to the secret key K , making an exclusive OR between the two random results $K_{iy'}$ and $K_{iz'}$: $K_i = K_{iy'} \text{ XOR } K_{iz'}$.

10 However, preferably and as depicted in Figure 7, the subkey K_i of the round Ti is not recalculated. The first random result $K_{iy'}$ is applied in place of the subkey K_i in an exclusive OR operation XOR with the data item 1 supplied by the permutation expansion operation EXP PERM. An intermediate result b' is
15 obtained.

By then effecting an exclusive OR XOR of this intermediate result b' with the second random result $K_{iz'}$, the output data item $b = \text{XOR}(1, K_i)$ is found.
20 The following operations are then performed in each round Ti , in order to calculate the parameter b from 1:

$$b' = 1 \text{ XOR } K_{iy'} \text{ and}$$

$b = b' \text{ XOR } K_{iz'}$, as shown for the first and second rounds in Figure 6.

25 In this way, the secret subkey itself is no longer used in calculating the enciphered message, but "random subkeys": the key is then protected before and during the execution of the cryptographic algorithm, since $K_{iy'}$ and $K_{iz'}$ being random and not known to the
30 external world of the component (or of the card), they

are liable to change at each new execution of the cryptography algorithm. It should be noted that, in the application of the countermeasure method according to the invention to the calculation and use of the subkeys, a random value is drawn only once, at the start of execution of the algorithm, before the operations on the secret key.

This second mode of applying the countermeasure method according to the invention to the secret key can advantageously be combined with the first mode of applying the countermeasure method to the calculation of the enciphered message proper, this combination making the countermeasure particularly effective.

The present invention applies to the DES secret key cryptography algorithm, for which examples of implementation have been described. It applies more generally to any secret key cryptography algorithm where the execution by the microprocessor of certain operations requires a bit by bit manipulation of data.

An electronic component 1 using a countermeasure method according to the invention in a DES secret key cryptography algorithm comprises typically, as shown in Figure 8, a microprocessor μP , a program memory 2 and a working memory 3. Means 4 of generating a random value are provided which, if reference is made to the flow diagrams in Figures 3 and 5, will supply the random values U and/or Y of the required size (32 bits for U, 64 bits for Y) at each execution of the cryptography algorithm. Such a component can particularly be used

in a smart card 5, in order to improve its resistance to tampering.

CLAIMS

1. A countermeasure method against attacks by differential analysis of current consumption in an electronic component using a cryptographic algorithm with a secret key K on an input message (M), characterised in that the execution of an operation (OPN) or of a sequence of operations comprising a bit by bit manipulation of an input data item (D), in order to supply an output data item (OPN(D)), comprises the following steps:
- drawing a random value, of a first random data item (U), with the same size as the input data item (D);
 - calculating a second random data item (V), effecting an exclusive OR between the input data item and the first random data item (U);
 - executing the operation (OPN) or the sequence of operations following on from the first random data item (U) and the second random data item (V), supplying respectively a first random result (OPN(U)) and a second random result (OPN(V));
 - calculating the output data item (OPN(D)) effecting an exclusive OR between the first and second random results.
2. A countermeasure method according to Claim 1, characterised in that it is applied to operations (EXP PERM, P PERM) relating to data calculated from the input message (M).
3. A countermeasure method according to either one of the preceding claims, characterised in that a

new random value (U) is drawn at each new execution of the said operation or sequence of operations.

4. A countermeasure method according to Claim 1, applied to an operation or a sequence of operations
5 (KEY PERM, SHIFT, COMP PERM) performed on the said secret key (K).

5. A countermeasure method according to Claim 4, the cryptography algorithm comprising several calculation rounds, and comprising a sequence of
10 operations on the secret key K in order to supply, at each round, (T_i), a corresponding subkey (K_i), a method characterised in that it is applied to the said sequence of operations in order to supply, at each round, a first random result (K_{iY}) and a second random
15 result (K_{iZ}).

6. A countermeasure method according to Claim 5, each round (T_i) an exclusive OR operation between the subkey (K_i) and an input data item (1) in order to supply an output data item (b), characterised in that
20 this operation is replaced by the following operations:

- calculating the exclusive OR between the said input data item (1) and the first random result (K_{iY}) in order to supply an intermediate result (b');
- calculating the exclusive OR between the said
25 intermediate result (b') and the second random result (K_{iZ}) in order to supply the said output data item (b).

7. A countermeasure method according to any one of Claims 1, 2, 3, 5 and 6, characterised in that a new random value (U or Z) is drawn at each new execution of
30 the cryptography algorithm.

9. An electronic security component implementing the countermeasure method according to any one of the preceding claims, characterised in that it comprises means (4) of generating a random value, a microprocessor (μ P), a program memory (2) and a working memory (3), the said means (4) supplying at least one random value (U) and/or (Y) of the required size, 32 bits for (U) and 64 bits for (Y), at each execution of the cryptography algorithm.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
24 août 2000 (24.08.2000)

PCT

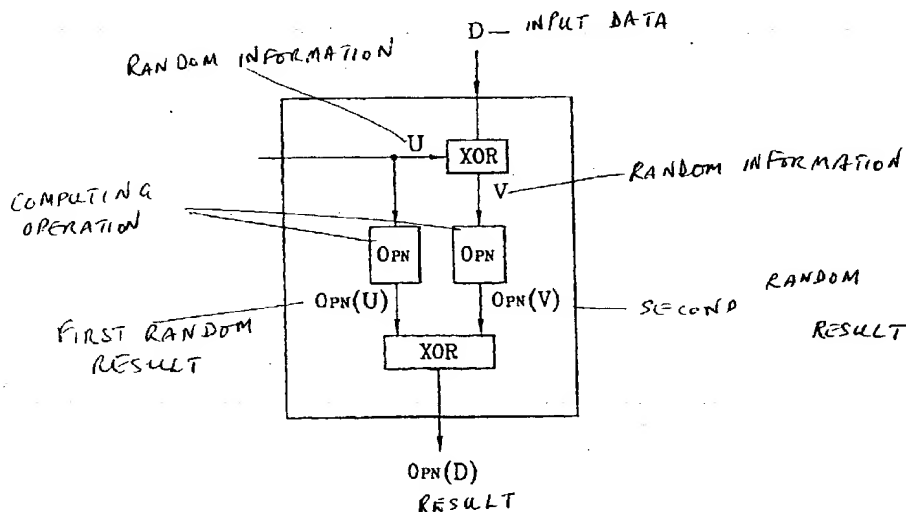
(10) Numéro de publication internationale
WO 00/49765 A3

- (51) Classification internationale des brevets⁷ : H04L 9/06
- (21) Numéro de la demande internationale : PCT/FR00/00130
- (22) Date de dépôt international : 20 janvier 2000 (20.01.2000)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité : 99/01937 17 février 1999 (17.02.1999) FR
- (71) Déposant (pour tous les États désignés sauf US) : GEMPLUS [FR/FR]; Avenue Du Pic de Bertagne, Parc d'activités de Gémenos, F-13881 Gémenos (FR).
- (72) Inventeurs; et
- (75) Inventeurs/Déposants (pour US seulement) : CORON, Jean-Sébastien [FR/FR]; 45, rue d'Ulm, F-75005 Paris (FR). FEYT, Nathalie [FR/FR]; 20, rue du Lieutenant J.P. Meschi, Bâtiment 6, F-13005 Marseille (FR). BENOIT, Olivier [FR/FR]; 22, rue Rastegue, F-13400 Aubagne (FR).
- (74) Mandataire : NONNEMACHER, Bernard; GEMPLUS, Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13881 Gémenos (FR).
- (81) États désignés (national) : AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU,

[Suite sur la page suivante]

(54) Title: METHOD FOR COUNTERMEASURE IN AN ELECTRONIC COMPONENT USING A SECRET KEY ALGORITHM

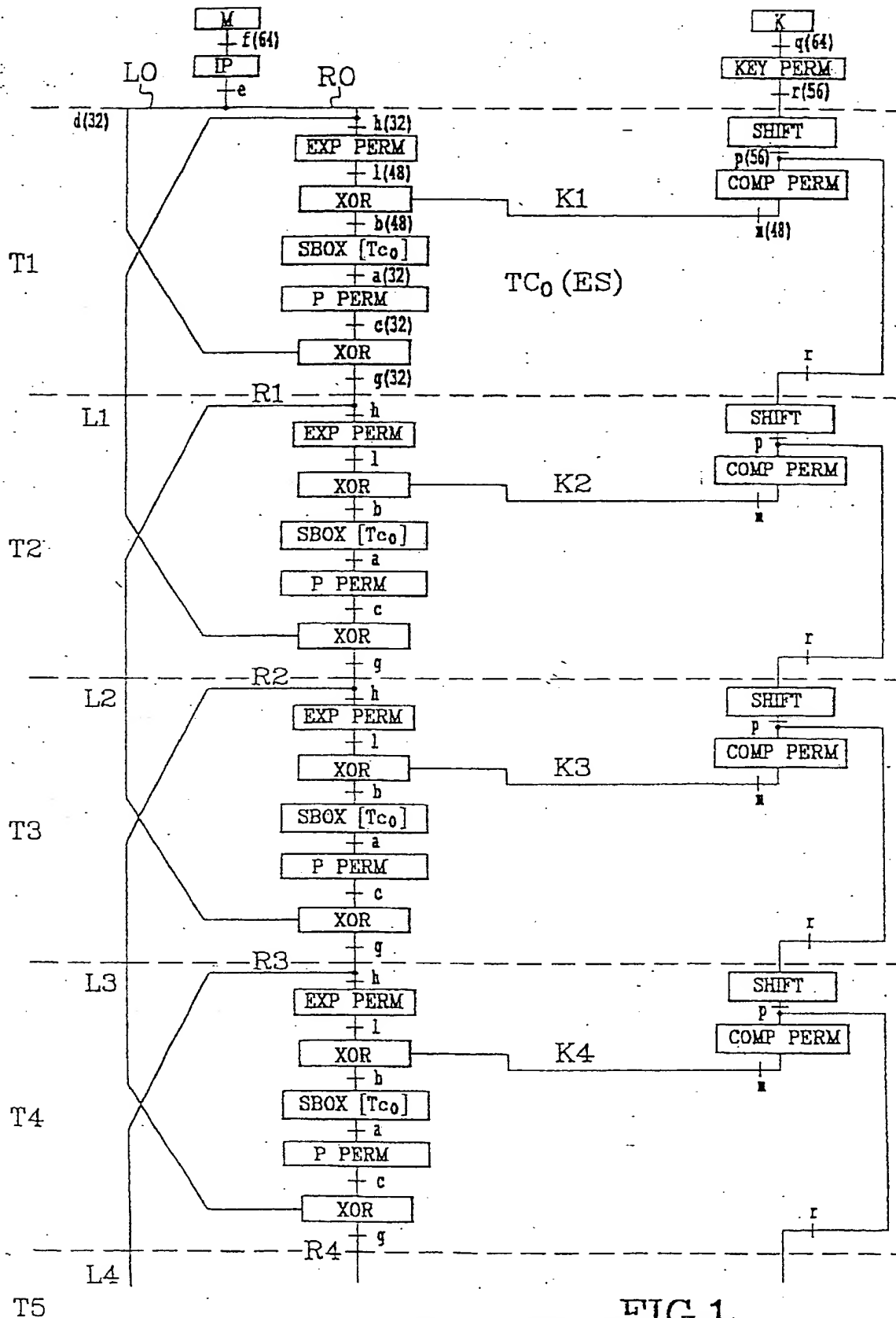
(54) Titre : PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE SECRETE



(57) Abstract: The invention concerns a countermeasure method in an electronic component using a secret key algorithm K on an input message M characterised in that the execution of an operation OP_N or of a sequence of operations comprising manipulating bit by bit an input information D, to supply an output information $OP_N(D)$, comprises the following steps: drawing a random value, of one first random information U, of identical size as the input information D; calculating a second random information V, by performing an exclusive OR between the input information and the first random information U; executing the operation OP_N or the sequence of operations successively to the first input information U and to the second random information V, supplying respectively a first random result $OP_N(U)$ and a second random result $OP_N(V)$.

[Suite sur la page suivante]

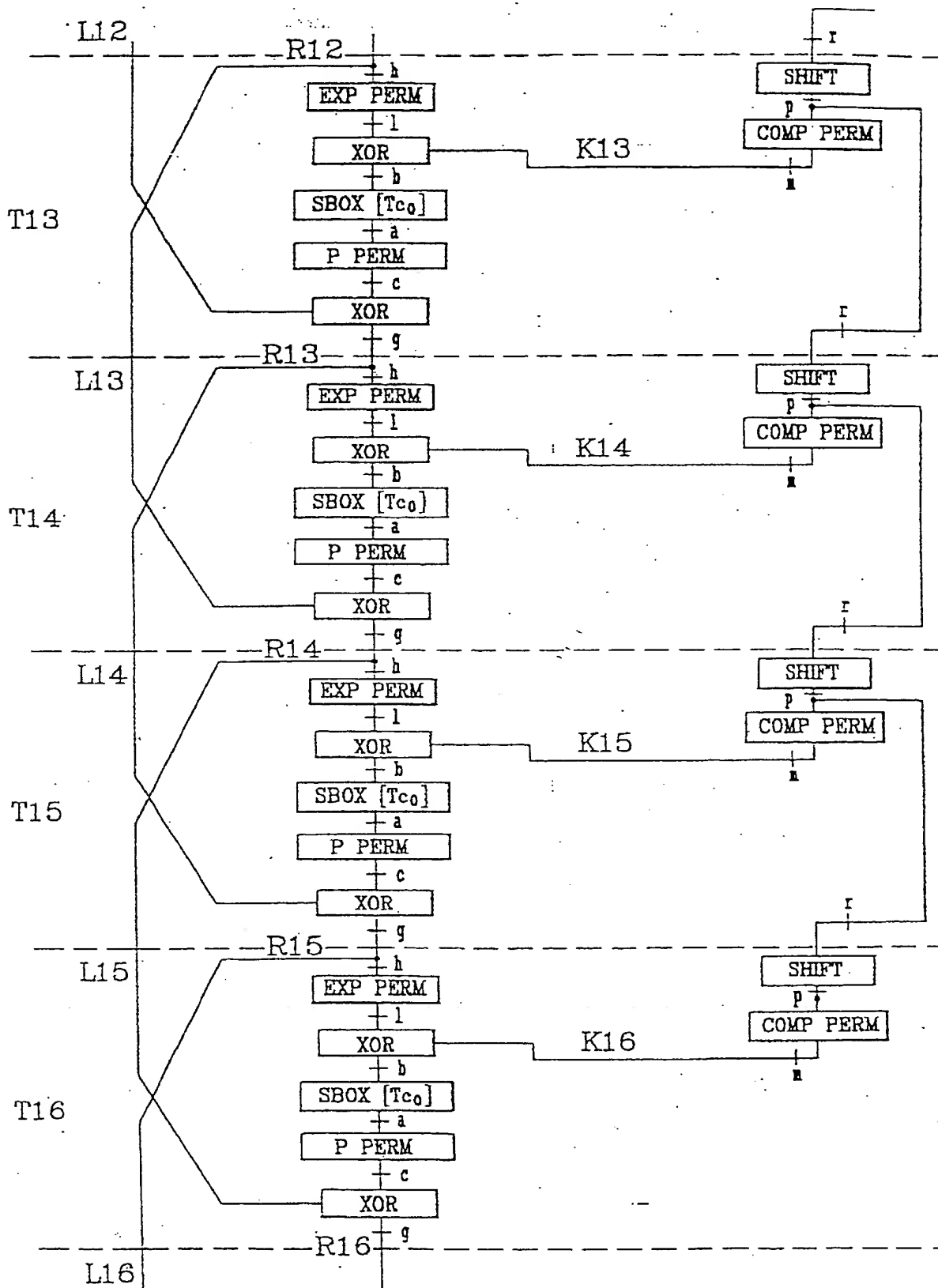
1/7

FIG. 1
FEUILLE MODIFI E

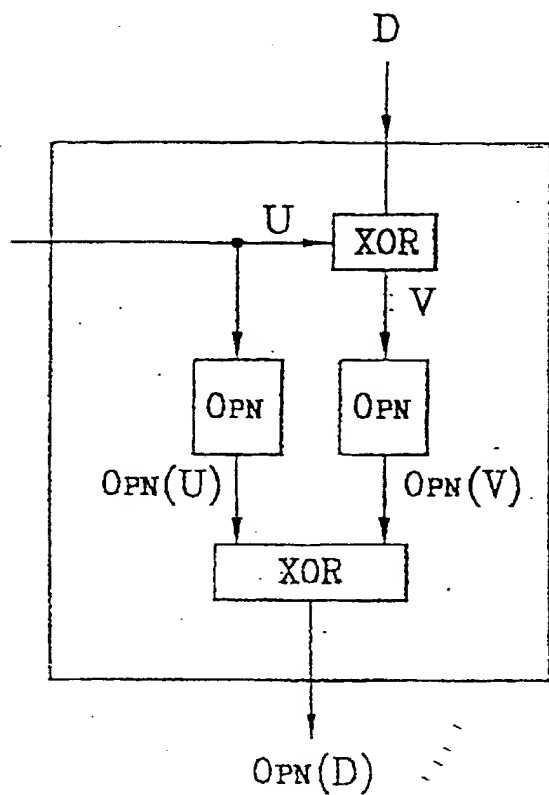
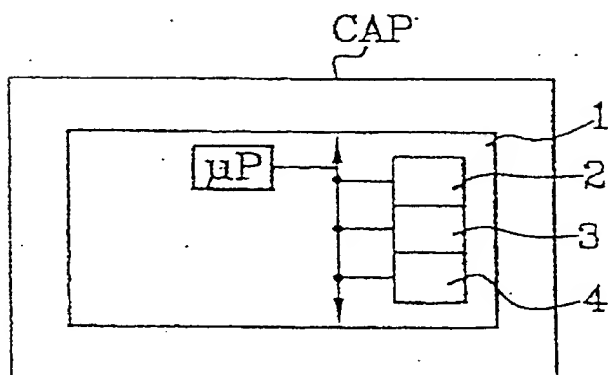
09/913884

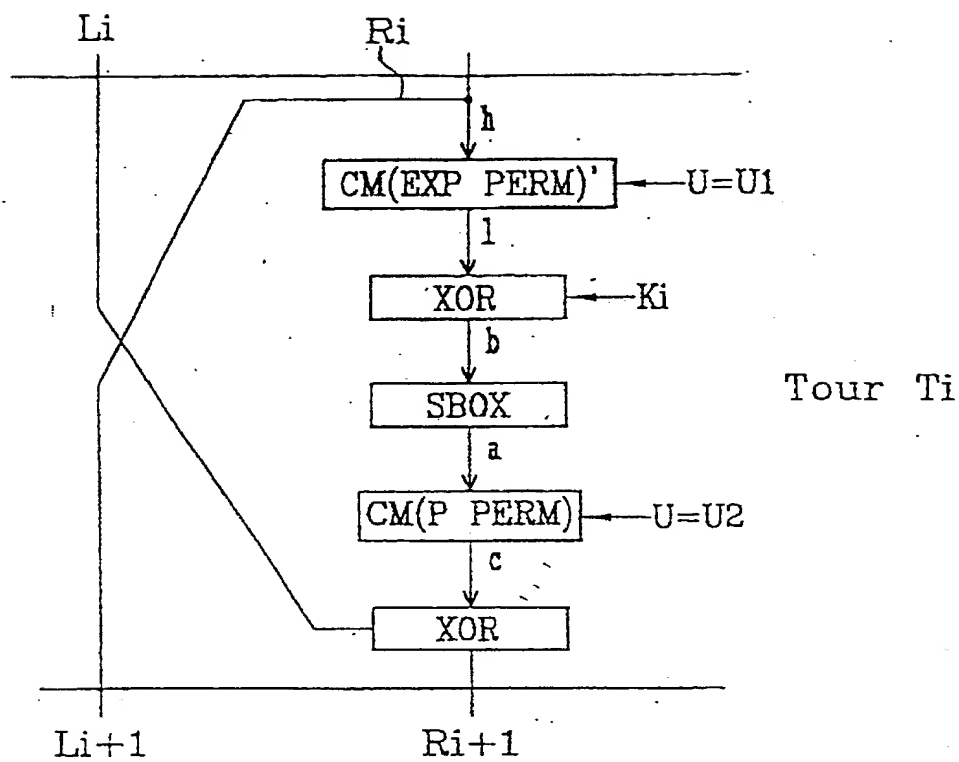
2/7

T12

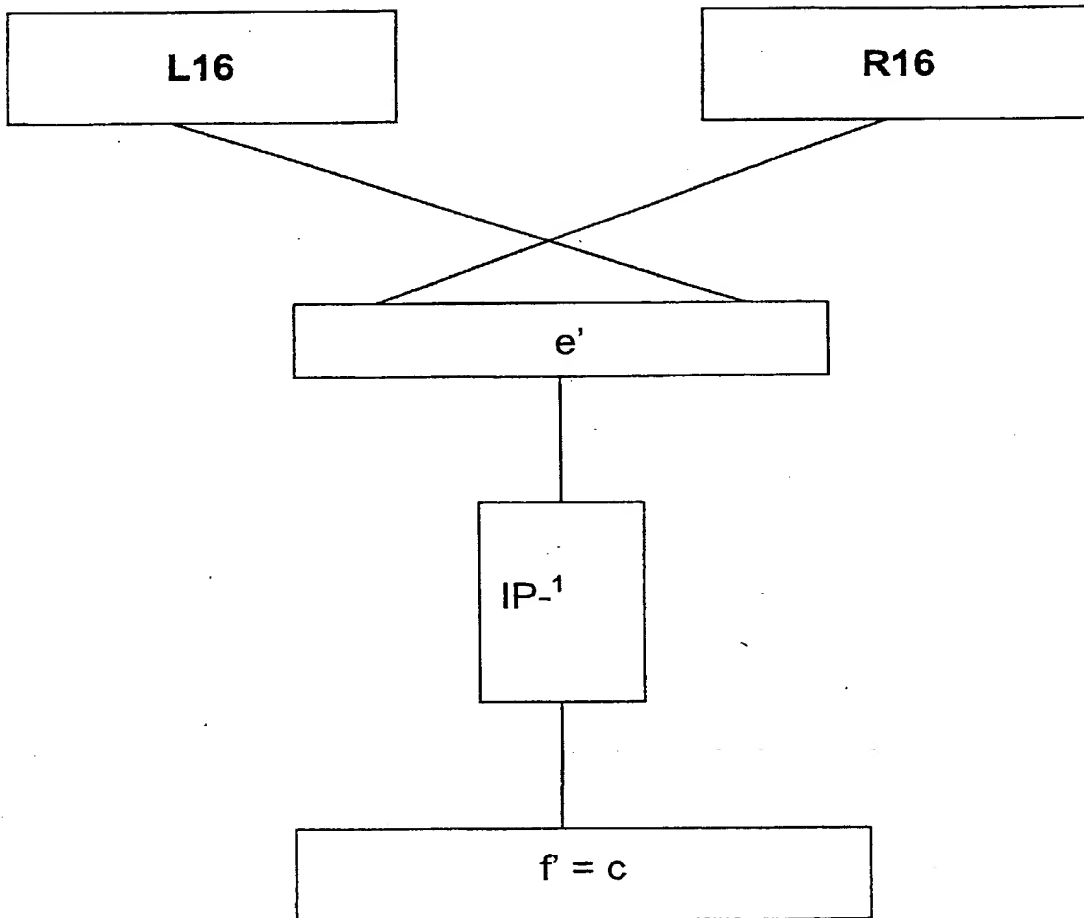


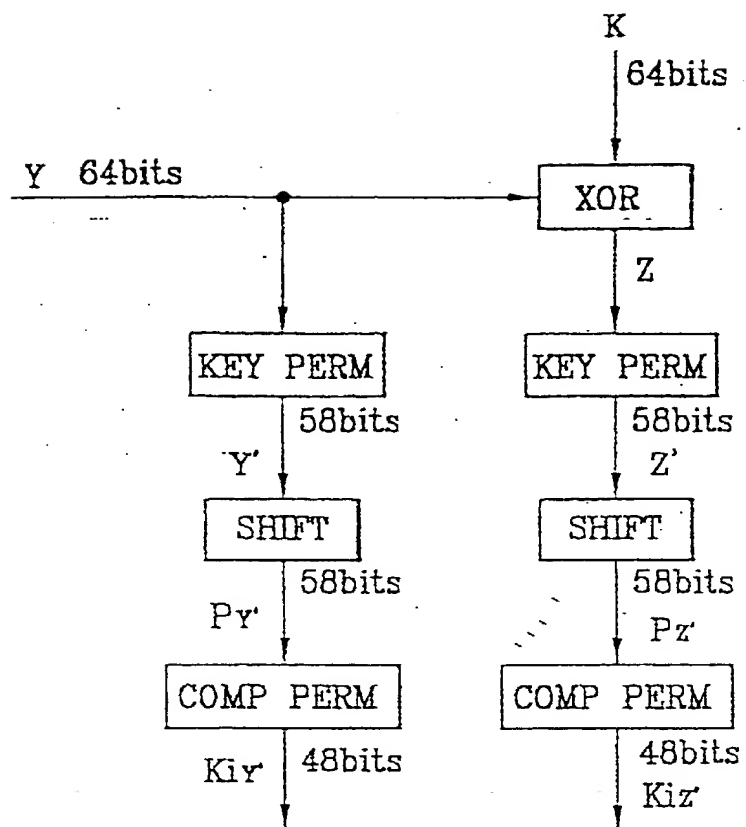
09/913884

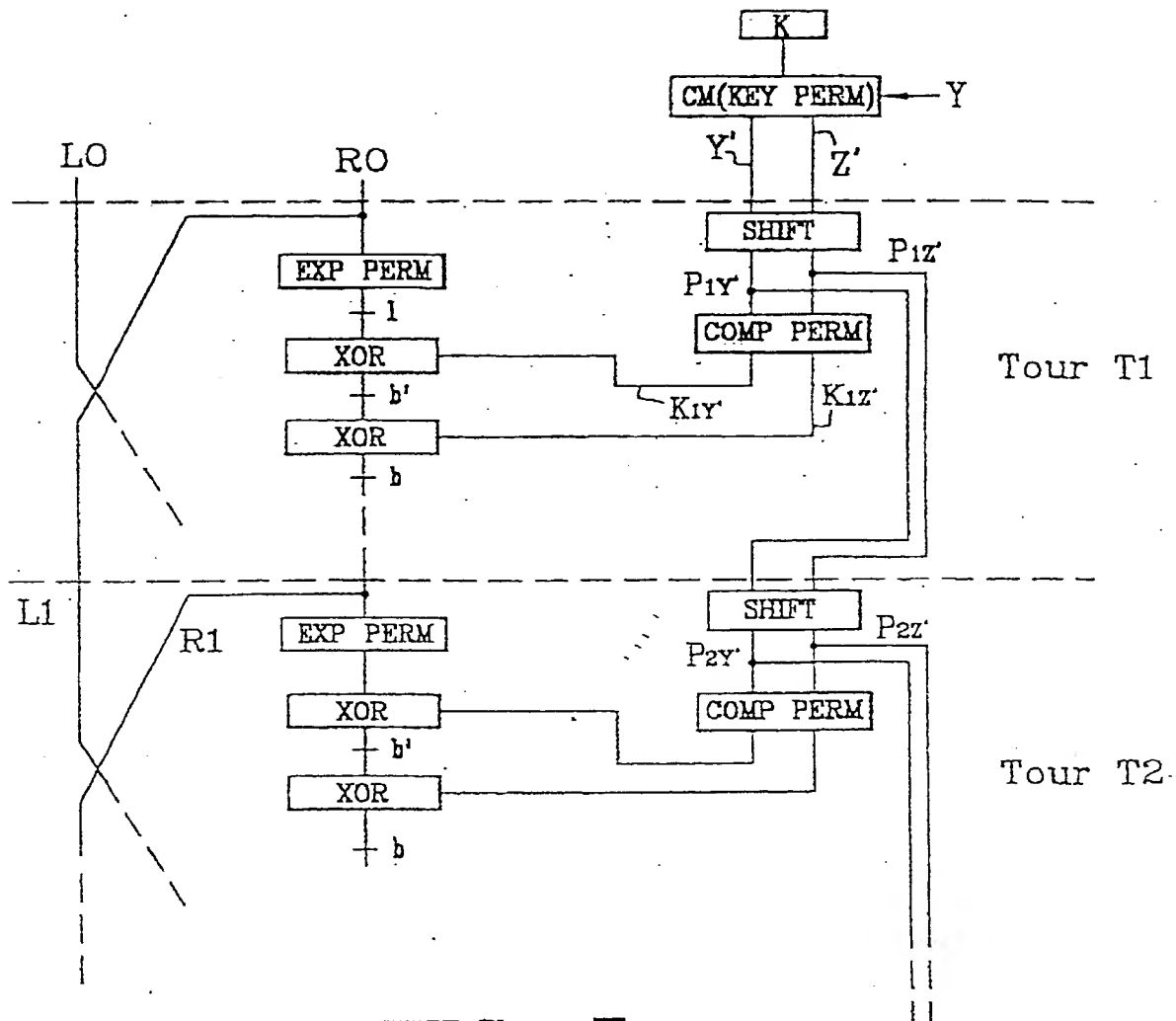
FIG.3FIG. 8

FIG.4

5/7

**FIG. 5**



**FIG. 7**

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY
(Includes Reference to Provisional and International (PCT) Applications)Attorney's Docket No.
032326-161

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I BELIEVE I AM THE ORIGINAL, FIRST AND SOLE INVENTOR (IF ONLY ONE NAME IS LISTED BELOW) OR AN ORIGINAL, FIRST AND JOINT INVENTOR (IF PLURAL NAMES ARE LISTED BELOW) OF THE SUBJECT MATTER WHICH IS CLAIMED AND FOR WHICH A PATENT IS SOUGHT ON THE INVENTION ENTITLED:

METHOD FOR COUNTERMEASURE IN AN ELECTRONIC COMPONENT USING A SECRET KEY ALGORITHM

The specification of which (check only one item below):

☒ is attached hereto.☐ was filed as United States Patent Application Number _____

and was amended on _____ (if applicable).

was filed as International (PCT) Application Number PCT/FR00/00130on 20.01.2000 (if applicable).
and was amended on _____

I HAVE REVIEWED AND UNDERSTAND THE CONTENTS OF THE ABOVE-IDENTIFIED SPECIFICATION, INCLUDING THE CLAIMS, AS AMENDED BY ANY AMENDMENT REFERRED TO ABOVE.

I ACKNOWLEDGE THE DUTY TO DISCLOSE TO THE U.S. PATENT AND TRADEMARK OFFICE ALL INFORMATION KNOWN TO ME TO BE MATERIAL TO PATENTABILITY AS DEFINED IN TITLE 37, CODE OF FEDERAL REGULATIONS, Sec. 1.56 (as amended effective March 16, 1992);

I do not know and do not believe the said invention was ever known or used in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to said application; that said invention was not in public use or on sale in the United States of America more than one year prior to said application; that said invention has not been patented or made the subject of an inventor's certificate issued before the date of said application in any country foreign to the United States of America on any application filed by me or my legal representatives or assigns more than six months prior to said application;

I hereby claim foreign priority benefits under Title 35, United States Code, §§ 119 (a)-(e) of any foreign application(s) for patent or inventor's certificate or of any International (PCT) Application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT International (PCT) Application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119:

COUNTRY (if PCT, indicate "PCT")	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119
France	99/01937	17 February 1999	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

(APPLICATION NUMBER)

(FILING DATE)

(APPLICATION NUMBER)

(FILING DATE)

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D)
(Includes Reference to Provisional and International (PCT) Applications)

 Attorney's Docket
 No. 032326-161

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States applications(s) or International (PCT) Application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to the patentability as defined in Title 37, Code of Federal Regulations § 1.56, which became available between the filing date of the prior application(s) and the national or international filing date of this application:

PRIOR U.S. APPLICATIONS OR INTERNATIONAL (PCT) APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. § 120:

U.S. APPLICATIONS		STATUS (check one)		
U.S. APPLICATION NUMBER	U.S. FILING DATE	PATENTED	PENDING	ABANDONED
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PCT APPLICATIONS DESIGNATING THE U.S.				
PCT APPLICATION NO.	PCT FILING DATE	U.S. APPLICATION NUMBERS ASSIGNED (if any)		
PCT/FR00/00130	20 January 2000			

I hereby appoint the following attorneys and agent(s) to prosecute said application and to transact all business in the U.S. Patent and Trademark Office connected therewith and to file, prosecute and to transact all business in connection with international applications directed to said invention:

William L. Mathis	17,337	Eric H. Weisblatt	30,505	Bruce T. Wieder	33,815
Robert S. Swecker	19,885	James W. Peterson	26,057	Todd R. Walters	34,040
Platon N. Mandros	22,124	Teresa Stanek Rea	30,427	Ronni S. Jillions	31,979
Benton S. Duffett, Jr.	22,030	Robert E. Krebs	25,885	Harold R. Brown III	36,341
Norman H. Stepno	22,716	William C. Rowland	30,888	Allen R. Baum	36,086
Ronald L. Grudziecki	24,970	T. Gene Dillahunt	25,423	Steven M. duBois	35,023
Frederick G. Michaud, Jr.	26,003	Patrick C. Keane	32,858	Brian P. O'Shaughnessy	32,747
Alan E. Kopecki	25,813	B. Jefferson Boggs, Jr.	32,344	Kenneth B. Leffler	36,075
Regis E. Slutter	26,999	William H. Benz	25,952	Fred W. Hathaway	32,236
Samuel C. Miller, III	27,360	Peter K. Skiff	31,917	Wendi L. Weinstein	34,456
Robert G. Mukai	28,531	Richard J. McGrath	29,195	Mary Ann Dillahunt	34,576
George A. Hovanec, Jr.	28,223	Matthew L. Schneider	32,814		
James A. LaBarre	28,632	Michael G. Savage	32,596		
E. Joseph Gess	28,510	Gerald F. Swiss	30,113		
R. Danny Huntington	27,903	Charles F. Wieland III	33,096		



21839

 and: _____
 Address all correspondence to:

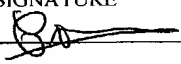
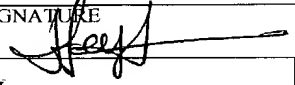
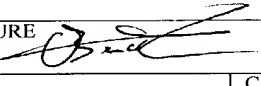
 James A. LaBarre
 BURNS, DOANE, SWECKER & MATHIS, L.L.P.
 P.O. Box 1404
 Alexandria, Virginia 22313-1404


21839

Address all telephone calls to: _____ at (703) 836-6620.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY (CONT'D) (Includes Reference to Provisional and International (PCT) Applications)	Attorney's Docket No. 032326-161
---------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------

100 FULL NAME OF SOLE OR FIRST INVENTOR Jean-Sebastien CORON	SIGNATURE 	DATE 12/12/2007
RESIDENCE (CITY & STATE/COUNTRY) 45 rue d'Ulm, 75005 Paris, FRANCE FRX	CITIZENSHIP French	
POST OFFICE ADDRESS (HOME ADDRESS) 45 rue d'Ulm, 75005 Paris, FRANCE		
200 FULL NAME OF SECOND JOINT INVENTOR, IF ANY Nathalie FEYT	SIGNATURE 	DATE 07/01/2002
RESIDENCE (CITY & STATE/COUNTRY) 20 rue du Lieutenant J.P. Meschi, Batiment 6, 13005 Marseille, FRANCE FRX	CITIZENSHIP French	
POST OFFICE ADDRESS (HOME ADDRESS) 20 rue du Lieutenant J.P. Meschi, Batiment 6, 13005 Marseille, FRANCE		
300 FULL NAME OF THIRD JOINT INVENTOR, IF ANY Olivier BENOIT	SIGNATURE 	DATE 19/12/2001
RESIDENCE (CITY & STATE/COUNTRY) 22 rue Rastegue, 13400 Aubagne, FRANCE FRX	CITIZENSHIP French	
POST OFFICE ADDRESS (HOME ADDRESS) 22 rue Rastegue, 13400 Aubagne, FRANCE		
FULL NAME OF FOURTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)	CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)		
FULL NAME OF FIFTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)	CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)		
FULL NAME OF SIXTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)	CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)		
FULL NAME OF SEVENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)	CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)		
FULL NAME OF EIGHTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)	CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)		
FULL NAME OF NINTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)	CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)		
FULL NAME OF TENTH JOINT INVENTOR, IF ANY	SIGNATURE	DATE
RESIDENCE (CITY & STATE/COUNTRY)	CITIZENSHIP	
POST OFFICE ADDRESS (HOME ADDRESS)		